Datenschutz-Compliance

Rolf H. Weber
Prof. Dr. iur., Rechtsanwalt
Telefon +41 58 258 10 00
rolf.weber@bratschi-law.ch

Compliance im Datenschutz bedeutet das Einhalten von internen und externen „Normen", die den Schutz von Informationen vor einer Zugänglichmachung an Dritte bezwecken.

1. Informationsbewirtschaftung

Die tägliche Erfahrung lehrt, dass in den Unternehmen immer mehr Daten anfallen und damit auch die Tendenz auflebt, diese Daten auszutauschen. Oft geht indessen vergessen, dass einerseits Vertraulichkeitsbedürfnisse bestehen, wenn die Daten einen Personenbezug aufweisen, und andererseits nicht alle Informationen zwingend auch alle Unternehmensbeteiligte interessieren. Zwecks Einhaltung gesetzlicher Geheimhaltungsregeln drängt es sich deshalb auf, unternehmensintern eine sinnvolle Informationskanalisierung vorzunehmen.

Abgesehen von spezifischen Geheimhaltungsregeln (Berufs-, Amts-, Bankgeheimnis) nimmt insbesondere das Datenschutzgesetz (DSG) mit seiner konkretisierenden Verordnung (VDSG) die Aufgabe wahr, die Sammlung und Verbreitung personenbezogener Informationen zu beschränken. Über das zum Teil eher abstrakte Schutzkonzept der gesetzlichen Ordnung hinaus erweist es sich indessen als unabdingbar, dass auch im Unternehmen selber sachspezifische Regeln ausgearbeitet und implementiert werden, die dazu beitragen, dass eine konkretisierte Umsetzung der Datenschutzvorgaben erfolgt.

Regulierungsaspekte sind die Voraussetzungen der Bereitstellung und Verarbeitung von Informationen, die Festlegung des Zugriffs auf Daten, die Verteilung von Daten innerhalb des Unternehmens, insbesondere bei Vorliegen multinationaler Geschäftsbeziehungen, und die Nachverfolgbarkeit des Datenflusses.

2. Compliance in Informationssystemen

Datenschutzrecht ist zu einem wesentlichen Teil auch Informationssicherheitsrecht. Faktisch geht es also darum, Sicherheitsvorkehren einzurichten, die verhindern sollen, dass Unberechtigte einen Zugriff auf geschützte Daten erlangen können. Prospektiv, zeitlich vor der Compliance, stellt ein gutes Risikomanagement ein sinnvolles Führungsinstrument dar.

Die Datensicherheit ist eine Aufgabe, die interdisziplinär anzugehen ist. Sicherheitsstrategien und Mechanismen zur Durchsetzung von Sicherheitseigenschaften lassen sich dabei unter verschiedenen Gesichtspunkten modellieren. In der Praxis sind zum Schutz von Informationen und ganzen Informationssystemen folgende Differenzierungen vorzunehmen:

- Nach funktionalen Kriterien ist eine Unterteilung in technische oder physikalische Sicherheitsmassnahmen und organisatorische Massnahmen (z.B. personelle und institutionelle Massnahmen, administrative Massnahmen, konzeptionelle Massnahmen) denkbar.

- Mit Blick auf die Wirkungsweise lässt sich differenzieren zwischen präventiven Massnahmen (vor Auftritt oder zur Verhinderung eines sicherheitsrelevanten Ereignisses), detektiven Massnahmen (beim Auftritt einer sicherheitskritischen Situation) und reaktiven Massnahmen (nach Eintritt eines Schadens).

Ein Unternehmen sollte über eine IT-Sicherheits-Policy und ein IT-Sicherheitskonzept verfügen; als Einzelaspekte anzusprechen sind die Festlegung der Zuständigkeiten, die Verfügbarkeit von Syste-

men, die Funktionssicherheit, die Kontinuität der Geschäftsabläufe, die Vertraulichkeit bzw. Geheimhaltung von Geschäfts- oder Kundendaten, die Klassifizierung von Informationen und der Umgang mit klassifizierter Information, die Datensicherung, die Integrität von Daten und Informationen, die Zurechenbarkeit von Informationen zu ihrem Urheber, die Kostenreduktion im Schadensfall, die Berichterstattung, die Kundenzufriedenheit, das Image und die Reputation des Unternehmens, die Festlegung der Risikoanalysemethoden und die Vorgabe grundsätzlicher Vorschriften hinsichtlich bestimmter sicherheitsrelevanter Anwendungen (wie etwa E-Mail, Nutzung mobiler Endgeräte, Softwareinstallation und Archivierung).

Gestützt auf solche Grundsätze lassen sich konkrete Richtlinien ausarbeiten, welche sich auf die einzelnen Einsatzbereiche beziehen (z.B. Datensicherung, Nutzung von Endgeräten, Umgang mit klassifizierten Dokumenten, Archivierung, Notfallmanagement usw.).

3. Regulatorische Schutzziele

Das Datenschutzgesetz nennt einzelne Schutzziele, die aber eine grosse Abstraktionshöhe aufweisen: Wer Daten sammelt und bearbeitet, hat sicherzustellen, dass die Daten (inhaltlich) auch richtig sind; die Datensammlung bzw. -bearbeitung hat unter Beachtung des Verhältnismässigkeitsprinzips und der Zweckgebundenheit (Beschränkung auf den Sachverhalt für relevante Daten) zu erfolgen (Art. 4 DSG). Diese allgemeinen Grundsätze, die zum Teil zwar eine gewisse Konkretisierung in der Rechtsprechung erfahren haben, sind im Unternehmen spezifisch umzusetzen. Dieser Vorgang beinhaltet, dass der Geltungsbereich von Bestimmungen klar umschrieben wird:

(i) Das Schutzziel der Vertraulichkeit von Informationen stellt sicher, dass weder Mitarbeiter noch Dritte bearbeitete Informationen im aktiven oder passiven Informationsfluss rechtswidrig zur Kenntnis nehmen oder IT-Systeme missbrauchen können.

(ii) Die Informationen müssen den Kriterien der Richtigkeit und Vollständigkeit Genüge tun; zu gewährleisten sind die Authentizität und die Integrität der Information, d.h. Daten müssen vollständig vorhanden und unverändert sein.

(iii) Die Verfügbarkeit der Informationen bezeichnet in der Informationssicherheitsdebatte die zulässige Ausfalldauer eines Schutzobjektes; weiter ist die Auffindbarkeit der Information sicherzustellen.

(iv) Nötig ist zudem die klare Zuordnung der Informationsbearbeitung zu einer bestimmten Person (Zurechenbarkeit); zu gewährleisten ist, dass die Informationen wirklich vom Benutzer oder von der angegebenen Person stammen.

(v) Schliesslich ist von Bedeutung, Änderungen der Informationen in einer Weise vorzunehmen, welche die Tatsache der Änderung erkennbar werden lässt (Nachvollziehbarkeit).

Art. 9 VDSG umschreibt die besonderen Massnahmen, die im Kontext der automatisierten Bearbeitung von Personendaten zu treffen sind, nämlich die Zugangskontrolle (lit. a), die Personendatenträgerkontrolle (lit. b), die Transportkontrolle (lit. c), die Bekanntgabekontrolle (lit. d), die Speicherkontrolle (lit. e), die Benutzerkontrolle (lit. f), die Zugriffskontrolle (lit. g) und die Eingabekontrolle (lit. h).

Die von einem Unternehmen entwickelten und für anwendbar erklärten Regeln sind auch auf der Zeitachse zu definieren: Ist die Regel jederzeit anzuwenden? Gilt die Regel vor einem bestimmten Ereignis? Ist die Regel nach einem bestimmten Ereignis zu beachten? Wird die Regel zwischen zwei Ereignissen angewendet?

Eine grosse Bedeutung kommt der Sicherstellung der effektiven Umsetzung der intern eingeführten Richtlinien zu; insbesondere müssen die Richtlinien verbindlichen Charakter aufweisen und es sind Instrumente vorzusehen (z.B. Weisungsbefugnisse gestützt auf eine klare Zuständigkeitsordnung), welche eine Überprüfung und Durchsetzung der Massnahmen und Vorgaben erlauben.

Hilfe bei der Formulierung von internen Richtlinien lassen sich den Checklisten entnehmen, die der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte erarbeitet hat. Als Beispiel ist auf die Rah-

menbedingungen der Benutzung des unternehmerischen Informationssystems für privaten Mailverkehr am Arbeitsplatz hinzuweisen.

4. Besonderheiten bei einem Outsourcing der Datenbearbeitung

Wird die Datenbearbeitung an ein Drittunternehmen ausgelagert, hat das Unternehmen sicherzustellen, dass dessen Datenbearbeitung in Übereinstimmung mit den gesetzlichen Vorgaben erfolgt (Art. 10a DSG). Die Verantwortung für die Datenbearbeitung verbleibt beim auslagernden Unternehmen. Zwecks Gewährleistung der gesetzlichen Vorgaben ist der Abschluss einer detaillierten Outsourcing-Vereinbarung unumgänglich. Checklisten und Vertragsmuster sind zwischenzeitlich vorhanden; mit Vorteil wird auf solche „Modelle“ zurückgegriffen.

Besondere Probleme ergeben sich, wenn eine Auslagerung ins Ausland erfolgen soll: In dieser Situation kommt Art. 6 DSG zur Anwendung, der verlangt, dass eine Datenbekanntgabe ins Ausland nur erfolgen darf, wenn die ausländische Gesetzgebung einen angemessenen Schutz bietet. Was unter dem Begriff des angemessenen Schutzes zu verstehen ist, lässt sich lediglich im Einzelfall nach den jeweils vorliegenden Umständen beurteilen. Zur Erleichterung eines Entscheids in solchen Situationen hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte gemäss Art. 7 VDSG eine Liste von Staaten mit einem angemessenen Datenschutzniveau erstellt.

Fehlt es im Empfängerstaat der Daten an einem angemessenen Schutzniveau, ist ein Outsourcing der Datenbearbeitung lediglich zulässig, wenn eine Einwilligung der betroffenen Person vorliegt, wenn vertragliche Sicherheitsvorkehren getroffen werden, die gewährleisten, dass die ausländische Dienstleistungserbringerin sich an die schweizerischen Datenschutzstandards hält oder wenn ein sog. Safe-Harbor-Agreement zur Anwendung gelangt, das den schweizerischen Datenschutzstandards zum Durchbruch verhilft.

Zürich Bahnhofstrasse 70, Postfach 1130, CH-8021 Zürich
Telefon +41 58 258 10 00, Fax +41 58 258 10 99
zuerich@bratschi-law.ch

Basel Gerbergasse 14, CH-4001 Basel
Telefon +41 58 258 19 00, Fax +41 58 258 19 99
basel@bratschi-law.ch

Bern Bollwerk 15, Postfach 5576, CH-3001 Bern
Telefon +41 58 258 16 00, Fax +41 58 258 16 99
bern@bratschi-law.ch

Zug Unter Altstadt 28, CH-6300 Zug
Telefon +41 58 258 18 00, Fax +41 58 258 18 99
zug@bratschi-law.ch

St.Gallen Vadianstrasse 44, Postfach 262, CH-9001 St.Gallen
Telefon +41 58 258 14 00, Fax +41 58 258 14 99
stgallen@bratschi-law.ch

www.bratschi-law.ch